Department of Homeland Security Daily Open Source Infrastructure Report for 3 April 2008

Current Nationwide

ELEVATED
Significant Risk of Terrorist Attacks

For info click here

- WBBM 2 Chicago reports emergency inspections were underway Wednesday morning on more than 50 United Airlines Boeing 777 aircraft. During a review of maintenance records, inspectors discovered that tests were not performed on one of the five bottles in the planes' fire suppression system. Until the tests are complete, the planes will not fly, United said. (See item **10**)
- According to the Associated Press, the U.S. Department of Agriculture plans to conduct a coordinated nationwide survey to determine whether an invasive moth that has been found in 12 California counties has spread to other states. State officials say the moth threatens more than 2,000 varieties of California plants and crops. (See item **17**)

DHS Daily Open Source Infrastructure Report Fast Jump

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *April 2, Sydney Morning Herald* – (International) **Experiment on clean coal to bury waste.** A "CLEAN COAL" experiment will begin in Australia today when the energy minister opens a demonstration plant that will inject up to 100,000 tons of carbon dioxide into a deep underground storage site in Victoria. The storage site, two kilometers under dairy country in the Otway basin, is part of the world's largest

demonstration plant burying carbon dioxide. The launch will be attended by energy officials from major greenhouse emitting countries including the U.S., Japan, South Korea, and India, along with coal, gas, and oil company executives who are here for the meeting of the Asia-Pacific Partnership on Clean Development and Climate. The Otway project is designed to show on a small scale that capturing carbon dioxide, shipping it by pipe, and storing it underground is possible without it leaking.
Source: http://www.smh.com.au/news/environment/experiment-on-clean-coal-to-bury-waste/2008/04/01/1206850910666.html

2. *April 2, Hess Corporation* – (International) **Easy oil 'to decline in a decade.'** The chief executive of Royal Dutch Shell said that he believes oil and gas reserves that are easy to exploit will reach their peak within the next decade. "It's becoming technologically expensive, capital intensive and lead times are growing longer," he said Tuesday during a seminar at the Center for Strategic International Studies. He added that certain countries would continue to have large supplies of conventional oil reserves but noted that they are likely to put a limit on the exploitation of their stocks. And the cost of development of harder-to-obtain oil resources would restrict growth, he added.
Source: http://www.hessenergy.com/common/NewsItem.aspx?ArticleId=18533397

3. *April 1, Reuters* – (North Carolina) **Eight protesters arrested at coal plant.** Eight protesters who locked themselves to bulldozers at a Duke Energy Corp. coal-fired power plant in North Carolina as part of a day of international actions on climate change were arrested on Tuesday. The Rutherford County Sheriff said the protesters were arrested for trespassing. The group was protesting the construction of a new coal unit, which would emit the greenhouse gas carbon dioxide. They entered company property but did not stop construction of the 800-megawatt Unit 6 at the Cliffside coal plant, said a spokesperson.
Source:
http://news.yahoo.com/s/nm/20080401/us_nm/coal_protest_duke_dc;_ylt=AgSVmiTTHW6ez22wt2S.vi0WIr0F

[Return to top]

Chemical Industry Sector

4. *April 1, ESS* – (National) **Terrorism attack and pandemic exercise at ESS EXPO.08 spotlights strategies and tools to safeguard U.S. chemical plants.** ESS, the leading provider of Environmental, Health and Safety (EH&S) and Crisis Management software for enterprise sustainability, announced Tuesday that it will sponsor a major chemical facility anti-terrorism exercise during ESS EXPO.08, where organizations will demonstrate the latest information technology tools for crisis management. ESS EXPO.08 will be held April 13-17, 2008 at the Wild Horse Pass in Phoenix. The exercise begins with a simulation titled Green Scorpion, in which terrorists gain access to a large chemical processing facility. Emergency teams will implement response strategies that are designed to stop the terrorists, free hostages, and prevent or mitigate damage to the facility and surrounding area. In addition, the exercise will also look at how the incident might be complicated by the simultaneous outbreak of a pandemic.

Providing a multi-hazard scenario will demonstrate why public and private organizations need a comprehensive emergency response strategy and the latest integrated information management tools. Emergency exercises are now required for certain facilities under the Chemical Facility Anti-Terrorist Standards (CFATS), a Department of Homeland Security (DHS) rule designed to identify and secure high-risk chemical facilities that present potential terrorist threats. An ESS crisis management expert will lead the exercise on Monday, April 14.
Source: http://biz.yahoo.com/bw/080401/20080401006732.html?.v=1

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

5. *April 1, Nevada Appeal* – (Nevada) **Medical equipment triggers alarm at Truckee CHP scales.** The Federal Bureau of Investigation responded to Interstate 80 in Truckee Tuesday morning after radiation was detected in a big rig at the truck scales, a Nevada County Sheriff's official reported. The radioactive material was detected by a radiation Geiger counter, spurring law enforcement from all over the region to respond in accordance to Homeland Security protocol. "The FBI flew in and there was law enforcement all over the place," he said. However, the scare was a false alarm: The radioactive material was coming from medical equipment hauled by the truck. The truck driver had forgotten to put the radioactive item on his list, triggering the response, he said.
Source: http://www.nevadaappeal.com/article/SS/20080401/NEWS/490158165

6. *April 1, Associated Press* – (New Mexico) **State reaches settlement with DOE over WIPP violation.** The New Mexico Environment Department says it has reached a $110,700 settlement with the U.S. Department of Energy's (DOE) Carlsbad field office. The settlement came over an errant waste drum sent to the DOE's nuclear waste repository near Carlsbad. The Waste Isolation Pilot Plant (WIPP) in June had accepted a drum of waste from Idaho National Laboratory for disposal although the drum contained liquid. The permit prohibits WIPP from accepting liquid waste because of the risks of leaks or potentially explosive materials. The state ordered the drum removed; it was returned to Idaho in mid-August.
Source: http://www.kdbc4.com/Global/story.asp?S=8102350&nav=menu608_2_1

[Return to top]

Defense Industrial Base Sector

7. *April 1, Defense News* – (National) **Boost-phase tracker hits test target: Raytheon.** December flight tests show that Raytheon has cleared another hurdle in its newest ballistic missile defense venture, said company executives. In the test, an Air National Guard F-16 fired an AIM-9X Sidewinder with the baseball-sized Network Centric Airborne Defense Element (NCADE) seeker on board. The test proved the NCADE's ability to acquire and track a ballistic missile in its boost phase. "The purpose of the test was not to intercept the missile; it was just to get close enough to get the plume and the

hardbody in the seeker's field of view so we could optimize the software," said a Raytheon executive. But intercept it did. "It hit north of the fins of the missile. That's the first significant intercept from an airborne platform," he said. NCADE will add an infrared seeker and a second-stage rocket motor built by Aerojet to Raytheon's ubiquitous Advanced Medium Range Air-to-Air Missile (AMRAAM), providing an affordable boost- and ascent-phase ballistic missile defense option for the U.S. Longer-range tests with the seeker and developmental propulsion system on the AMRAAM airframe will come by the end of 2009, he said. Raytheon has also outlined a program plan with the Missile Defense Agency that would put 20 missiles on the ramp within four years of becoming a program of record, he said.
Source: http://www.defensenews.com/story.php?i=3457386&c=AME&s=AIR

[Return to top]

Banking and Finance Sector

8. *April 1, WCVB 5 Boston* – (Massachusetts) **Environmental protesters chain selves to bank.** Environmental activists concerned about global warming chained themselves to the front entrance of the Bank of Boston building on in Boston early Tuesday. They said they were protesting the bank's funding of coal and energy companies, which they said are among the worst contributors to climate change. The April Fool's prank was part of the Fossil Fools Day of Action, which took place in coordination with 100 other rallies, protests and other acts of civil disobedience around the country, the group said. They said the protests are designed to "challenge and disrupt the fossil fuels industry," which some scientists say is primarily responsible for global warming. The protesters claim Bank of America has loaned more than $144 billion to companies such as Massey Energy, Arch Coal and Peabody Energy, which engage in strip mining and mountaintop removal coal mining. The activists said coal-burning power plants are responsible for 40 percent of U.S. greenhouse gases that cause global warming. The Fossil Fools Day of Action was called for by Rising Tide North America, Rainforest Action Network, and the Energy Action Coalition.
Source: http://www.thebostonchannel.com/news/15761552/detail.html

9. *April 1, Stories in the News* – (National) **BBB warns consumers against getting instant tax refunds.** Instant tax refunds, also called Refund Anticipation Loans (RAL), are short-term loans given to the consumer immediately after the tax preparer files their taxes. The tax preparer will then receive the filer's refund check two to three weeks later from the IRS. The effective annualized interest rate for instant tax refunds range from 50 to nearly 500 percent, according to the National Consumer Law Center (NCLC). Some tax preparers further gouge consumers by tacking on administrative fees. According to the NCLC, consumers took out more than nine million RALs in 2006 paying more than $990 million in fees. "Taxpayers who want to get their hands on their tax refund money right away need to keep in mind that an instant refund can cost more than it helps," said the president and CEO of the BBB serving Alaska, Oregon and Western Washington. "RALs are based on anticipated tax refunds. If consumers end up getting less money back than predicted, they will owe the money loaned plus hefty fees and fines if they don't pay off the RAL on time." Instant refunds came under scrutiny in January 2008.

The IRS issued a request for comments regarding regulations and restrictions governing RALs-particularly given the bad effect the practice has on low-income households.
Source: http://www.sitnews.us/0408news/040108/040108_bbb.html

[Return to top]

Transportation Sector

10. *April 2, WBBM 2 Chicago* – (National) **United grounds 52 planes for emergency inspection.** Emergency inspections are underway Wednesday morning on more than 50 United Airlines Boeing 777 aircraft. United says during a review of maintenance records, inspectors discovered that tests were not performed on one of the five bottles in the planes' fire suppression system. That mistake was voluntarily reported to the Federal Aviation Administration, United said. United officials said they are in the process of checking the fire suppression systems, which are regularly tested before each flight. Until the tests are complete, the planes will not fly, United said. Some delays were reported in parts of the country as altimeters were checked out.
Source: http://cbs2chicago.com/local/united.airlines.inspection.2.690121.html

11. *April 2, Sydney Morning Herald* – (International) **Govt. to consider more laser restrictions.** The Australian federal government will receive recommendations this week on how to curb laser attacks on airplanes. NSW police are calling for lasers to be regulated, not banned. The Australian Customs Service, Australian Federal Police, ASIO and other government agencies have begun compiling suggestions for tougher restrictions on laser pointers. Their meeting on Wednesday followed reports to police of a laser being shone from Sydney's Bossley Park area at a plane about 9.30pm on Tuesday. The plane, which was traveling from Cairns to Sydney's Kingsford Smith Airport, landed without incident and no one was injured. Six planes were also forced to alter their flight paths and delay landings into Sydney after a coordinated attack by four green lasers last Friday. The Federal Home Affairs minister said the most recent laser attack had increased the government's desire to act.
Source: http://news.smh.com.au/govt-to-consider-more-laser-restrictions/20080402-231m.html

12. *April 1, Associated Press* – (National) **Feds call for alerts on all air gliders.** All gliders should be required to operate with devices that alert air traffic controllers and other aircraft to their presence, federal regulators recommended Tuesday, citing 60 near-collisions over the past two decades. Gliders and other aircraft without engine-driven electrical systems are exempt from a rule the Federal Aviation Administration imposed in 1988 requiring transponders for aircraft that operate near primary airports and in airspace above 10,000 feet. The chairman of the National Transportation Safety Board recommended in a March 31 letter to the board that the glider exemption be eliminated in part because of an NTSB investigation into a collision between a glider and a private jet about 40 miles southeast of Reno in August 2006. Many gliders object to required use of transponders, saying they are expensive and energy-consuming. Of the 60 near mid-air collisions from 1988 to 2007, nine occurred in northern Nevada. That is due primarily to the large number of gliders that fly along the Sierra's eastern front where

thermal air flows create what enthusiasts describe as "world-class" gliding conditions. The NTSB concluded that "transponders are critical to alerting pilots and controllers to the presence of nearby traffic, so that collisions can be avoided and that gliders should not be exempt from the transponder requirements." The FAA has 90 days to respond to the NTSB's recommendations, a FAA spokesman said.
Source: http://ap.google.com/article/ALeqM5gJIJpMrPdf9TGKSpP-PvoNVHo5yQD8VPD7K00

13. *April 1, WKMG 6 Orlando* – (Florida) **Passenger at Orlando Airport had bomb materials, literature in bag.** A Jamaican man behavior specialists spotted acting suspiciously was detained and arrested after components used to make pipe bombs, unknown liquids and bomb-making literature were found in his luggage at Orlando International Airport. Officials said federal behavior identification agents noticed something about the man's body language that prompted officers to move in near the Virgin Atlantic and Jamaica Airlines ticket counters Tuesday afternoon. The passenger was immediately taken into custody and a portion of the Terminal A in front of Virgin Atlantic was closed to passengers. During a search of his luggage, airport authorities found two galvanized pipes, end caps, two small containers containing BBs, batteries, two containers with an unknown liquid and bombing making literature, FBI officials said. Only 11 flights were affected during the incident. TSA officials said flight operations were operating normally and security checkpoints were open Tuesday night.
Source: http://www.local6.com/news/15762829/detail.html

14. *April 1, Aviation News* – (National) **TSA unveils checkpoint of the future.** The Transportation Security Administration this week unveiled plans for its security checkpoint of the future. The agency is expected to launch a prototype at Baltimore-Washington International soon. It will then introduce individual components of the system at various other airports. In describing the planned system, TSA said that three elements will comprise the checkpoint evolution – people, process and technology. The agency said that the future will require that more officers specially trained in behavior detection and document checking be deployed to identify people that intend to do harm, not just waiting to find prohibited items in a carry-on bag. In addition, the checkpoint process will be improved, "including better signs to tell you what's going on at the checkpoint and why, and what you need to do at various stages," TSA said. For the technology upgrade, TSA said, "We don't have the end-all-be-all machine yet, but there are some technologies we will be installing in many airports throughout the year that are an improvement to what currently exists, including multi-view X-ray for carry-on bags and whole body imaging for passengers."
Source: http://www.aviationnews.net/?do=headline&news_ID=153134

15. *April 1, Aviation News* – (National) **FAA: Controller hiring on schedule.** The Federal Aviation Administration is on schedule to hire and train nearly 17,000 air traffic controllers over the next decade, the agency said, adding that it hired more than 1,800 controllers last year and expects to hire nearly 1,900 in fiscal year 2008. The details are contained in the Controller Workforce Plan released on Tuesday. FAA said that recent data show key improvements in training methods lowered the training time to become a

fully certified controller from an average of three to five years to an average of two to three years. Separately, FAA and the National Air Traffic Controllers Association signed an agreement to create an Air Traffic Safety Action Program, designed to foster a voluntary, cooperative, non-punitive environment for the open reporting of safety of flight concerns by FAA employees.
Source: http://www.aviationnews.net/?do=headline&news_ID=153133

[Return to top]

Postal and Shipping Sector

16. *April 1, WCPO 9 Cincinnati* – (Kentucky) **Hazmat called to IRS building in Covington.** The IRS building in Covington, Kentucky, has returned to normal operations after a suspicious substance was found Tuesday morning. Boone County Hazmat crews were called to the building after a substance was found in an envelope. Officials are expected to announce what the substance was. The building was not evacuated and no injuries were reported.
Source: http://www.kypost.com/content/wcposhared/story.aspx?content_id=e08eaaf4-23fd-4847-a1ab-7b697857dabb

[Return to top]

Agriculture and Food Sector

17. *April 1, Associated Press* – (California) **USDA schedules national survey to track invasive moth.** Federal officials plan to conduct a coordinated nationwide survey to determine whether an invasive moth that has been found in 12 California counties has spread to other states. The U.S. Department of Agriculture and state agriculture officials ordered aerial spraying of a pesticide along the central coast last year to combat the Australian light brown apple moth. State officials say the moth threatens more than 2,000 varieties of California plants and crops. USDA's Director of Emergency Management says in June the agency will conduct its first targeted survey in all 50 states and Puerto Rico aimed at detecting the moth. Opponents of the moth spraying are calling for the campaign to halt while scientists do a full study of its impact on human health.
Source: http://www.mercurynews.com/breakingnews/ci_8773005

18. *April 1, CIDRAP News* – (National) **USDA names chicken plants with Salmonella problems.** As expected, the U.S. Department of Agriculture (USDA) last week began publishing the names of broiler chicken plants that have had trouble with Salmonella, listing 21 facilities where more than 10 percent of samples were found contaminated in recent tests. Only two plants actually failed to meet the USDA's standard for Salmonella in chicken: a maximum of 20 percent of samples contaminated. At the other 19 plants, between 10 percent and 20 percent of recent samples had Salmonella, according to the USDA Food Safety and Inspection Service (FSIS). The plants listed are in 12 states and Puerto Rico. The two that failed the standard are a Pilgrim's Pride Corp. facility in Ellijay, Georgia, and a Tyson Foods Inc. plant in Center, Texas, according to the FSIS.

The USDA had said in January that it would begin listing facilities with higher Salmonella rates on March 28. The move is part of a control initiative the USDA first announced about two years ago, after several years of increasing contamination rates. About 16 percent of broiler chicken samples tested positive for Salmonella in 2005. The initiative includes a "risk-based" sampling program, in which FSIS focuses more of its sampling on plants that have higher Salmonella levels.
Source: http://www.cidrap.umn.edu/cidrap/content/fs/food-disease/news/apr0108salmo.html

19. *March 31, Foodconsumer.org* – (National) **JARD recalls fresh cut fruit products with cantaloupe.** A company on March 28 issued a recall of selected fresh cut fruit products produced with potentially Salmonella-contaminated cantaloupe. Earlier, the Food and Drug Administration issued a public alert saying cantaloupe from Agropecuaria Montelibano may be contaminated with Salmonella and all products are to be retained at borders for inspection. On March 26, 2008, JARD marketing was requested by its supplier T. M. Kovacevich International Inc, to recall the products produced with affected cantaloupe. Recalled foodservice products are packed in plastic pails or jars, and retail products are packed in plastic cups and trays. Products being recalled were distributed in Maine, New Hampshire, Vermont, Massachusetts, Connecticut, Rhode Island, New York, New Jersey, and Pennsylvania. Food service products containing cantaloupe packed in plastic pails and jars include: Pebble Beach, Festival Of Fruit, Cornucopia Sweet, Jambo Chef, Fowler Fruit Mix, Instantwhip, Syracuse Banana. and City Line Food Dist. Recalled pails are coded with an expiration date from "Exp Apr 7, 2008" to "Exp Apr 22, 2008" or with a Julian Code of "08067" to "08082". Plastic jars being recalled are coded with an expiration date of "Exp Apr 22, 2008" to "May 7, 2008" or with a Julian Code of "08067" to "08082". Retail products with cantaloupe packed in plastic cups and trays include: Frosty Fresh, Fresh Hand Cut, Fruit On The Go, Highland Park, Bruegger's Bagels, Sid Wainer & Son, Hannaford Brothers, and Garden Highway Plant # P-005. Recalled plastic cups and trays are coded with a sell by date of "3/29/08" or earlier. The FDA said officials are unaware of any illness associated with any products containing cantaloupe sold by JARD Marketing Corp. or its distributors.
Source:
http://foodconsumer.org/7777/8888/R_ecalls_amp_A_lerts_3/033103242008_JARD_recalls_fresh_cut_fruit_products_with_cantaloupe.shtml

[Return to top]

Water Sector

20. *April 1, KAIT 8 Jonesboro* – (Arkansas) **Broken levee threatens SouthSide water supply.** All through last week's flooding the water treatment plant functioned as it was supposed to. But when the waters receded, workers realized how close they had come to disaster. What they found was that their ten foot high levy along the river road was completely gone. The manager of the Southside Public Water Authority said, "This river begin from this flood to wallow out the bank on both sides of our intake facility here and for about 13/14 hundred feet or so further down the river here and if we don't get it

stabilized as quickly as possible I fear that we could be in major problems on any kind of future event like that." This kind of assault by the river is what the manager fears most since their 16-inch raw water line and power cables run parallel to the river. He said, "A major cut it could expose enough of it 30, 50, 60, 100 feet of it where it literally just falls into the river." A disaster of that scale would mean the homes that get their fresh water from the plant could lose their supply of water for an extended period. For now, holes have been filled in on the levee and the Army Corp of Engineers has been contacted for help.
Source: http://www.kait8.com/Global/story.asp?S=8103611&nav=0jsh

[Return to top]

Public Health and Healthcare Sector

21. *April 2, San Francisco Chronicle* – (National) **AIDS drug tied to heart attack risk, study says.** Patients who take the widely prescribed AIDS drug abacavir run nearly double the risk of heart attack compared with those who take other antiviral medications, according to a major study conducted in the United States, Europe, and Australia. The unexpected finding, which was released at a scientific meeting in February and published online by the journal Lancet on Tuesday, creates a quandary for HIV-positive patients and their physicians. Abacavir has run into trouble just as it was becoming one of the most important "backbones" of various three-drug combinations that keep HIV in check. As a result of the findings, the Food and Drug Administration on Thursday posted a notice that it was reviewing whether to take regulatory action. However, the agency emphasized that it had not concluded that the drug was responsible for the higher heart attack rate, nor was it advising doctors to stop prescribing it. Abacavir won FDA approval in 1998, and sales of its various formulations have topped $1 billion in recent years. In January, a federal panel that sets treatment guidelines recommended that the drug, combined with the antiviral 3TC and sold as Epzicom, be considered a "preferred choice" for patients taking AIDS drugs for the first time.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/04/02/MNE2VU4TF.DTL

22. *April 2, Agence France-Presse* – (International) **S. Korea reports suspected bird flu outbreak.** Korean officials sealed off a poultry farm after some 2,400 chickens died in a suspected bird flu outbreak in South Korea, the government said on Wednesday. Preliminary tests on chickens that died at a farm in Gimje, 260 kilometers southwest of Seoul, pointed to a suspected avian flu case, the agriculture ministry said. Some 2,400 chickens out of about 150,000 birds on the farm died between Saturday and Tuesday. The owner began reporting the deaths to health authorities on Monday. Detailed results were expected to be announced Friday.
Source: http://www.straitstimes.com/Latest+News/Asia/STIStory_223085.html

23. *April 2, All Headline News* – (International) **Donated liver, pancreas from cancer patient kills recipients.** Two of four patients who received donated organs from a boy whose death was belatedly diagnosed as caused by lymphoma cancer have died while two others survived after the timely removal of the diseased organs. The rare incident in

2007 was reported in the January issue of the American Journal of Transplantation. According to the report, the parents of 15-year-old organ donor decided to donate the liver, pancreas, and kidneys of their son immediately after his death in March 2007 from what doctors at the Stony Brook University Medical Center believed was bacterial meningitis. The parents sought an autopsy of their dead son's brain before the organs were extracted. The autopsy results, which came one month after the boy's death, indicated that the victim died from a rare lymphoma cancer.
Source: http://www.allheadlinenews.com/articles/7010510530

Government Facilities Sector

24. *April 2, Daily Press* – (Virginia) **Langley gates getting security upgrades.** Entrance gates to Langley Air Force Base in Hampton, Virginia, will have temporary closures and restrictions this week while security barriers are worked on, according to the Air Force. From Friday at 11 p.m. to Saturday at 6 a.m., the King Street Gate will be closed and the West Gate will have various lane restrictions.
Source: http://www.dailypress.com/news/local/dp-local_militarybrfs_04022apr02,0,5680083.story?track=rss

[Return to top]

Emergency Services Sector

25. *April 1, IDG News Service* – (International) **IBM fine-tunes model for disaster management.** IBM's research laboratories in the U.S. and India have fine-tuned technology to help model and manage catastrophes such as natural disasters and infectious disease pandemics. The new enhancements are to a budgeting system being developed by IBM, starting from 2003, for managing natural disasters, with a focus on better preparedness for future uncertain disaster scenarios. The optimization models and algorithms were initially prototyped on a large U.S. government program, to deploy a large number of critical resources to a range of disaster scenarios, said the lead researcher in the analytics and optimization research team at IBM India Research Laboratory in Delhi, India. That system, however, produced only a single solution for each scenario. The enhancements include a decision-support system so that a range of alternatives can be generated for each disaster scenario, IBM said Tuesday. A model that supports multiple criteria can be used effectively where there is contention over resources, such as when there is more than one disaster competing for resources, according to the lead researcher.
Source:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=9074060&taxonomyId=17&intsrc=kc_top

[Return to top]

Information Technology

26. *April 2, CIOL News Reports* – (National) **Email security threats impacting businesses worldwide.** Webroot, a leading provider of security solutions for the consumer, enterprise and SMB markets, has released its latest research report, "State of Internet Security: Protecting Business Email" The report reveals the significant impact that rapidly growing email security threats, in size and volume, are having on businesses worldwide and underscores the need for a multi-layered approach to Internet security. "The battle against spam is an on-going struggle for many organizations with spammers continuing to present a serious and costly threat to most businesses. In 2008, we estimate there will be over 42,000 spam emails for every single business email account, or about 116 per day. And, because spammers are working at beating conventional filters with images and attachments, the size of spam has grown 60 percent since 2004," said Webroot's Chief Operations Officer. "The size and volume of these spam attacks is largely due to the partial success of current filtering defenses that now make spamming success a numbers game. It's clear why first-generation defenses such as appliances and server-based software are struggling to keep up." Along with the rapid growth in spam, there is a similarly rapid growth in malware. Industry research shows that malware jumped from about 50,000 variants in 2004 to 5.5 million in 2007.
Source: http://www.ciol.com/SMB/News-Reports/Email-security-threats-impacting-businesses-worldwide/2408104955/0/

27. *April 2, ars technica*– (International) **Report: boot sector viruses and rootkits posed for comeback.** Security firm Panda Labs has released its malware report for the first quarter 2008. The report covers a number of topics and makes predictions about the types of attacks we may see in the future. Forecasting these trends is always tricky – no one expected the Storm Worm to explode when it did – but Panda's prediction that we may see a rise in boot sector viruses is rather surprising. Thus far, adware, trojans, and miscellaneous "other" malware including dialers, viruses, and hacking tools have captured the lion's share of the "market" as it were. These three categories account for 80.55 percent of the malware Panda Labs detected over the first quarter. Password-stealing trojans are still a growing market, and the report cautions users, as always, to be careful of their banking records. The monetization of the malware market, the prevalence of JavaScript/IFrame attack vectors, and the growing number of prepackaged virus-building kits are all issues that the report raises. Also, social engineering-based attacks are both dangerous and effective, and social networks, particularly those based around Web 2.0, are often tempting attack targets.
Source: http://arstechnica.com/news.ars/post/20080402-report-boot-sector-viruses-and-rootkits-posed-for-comeback.html

28. *April 1, Computerworld* – (National) **New exploit targets corporate CA users.** An exploit specifically targeting corporate Computer Associates users has been created some three weeks after a critical vulnerability was identified. The attack uses an ActiveX Control buffer overflow vulnerability present in 21 CA products, including BrightStor ARCServe Backup for Laptops and Desktops, Unicentre Remote Control, Software Delivery, Asset Management, Desktop Management Bundle, and Desktop

Management Suite. The exploit was rated as critical by the French Security Incident Response Team (FSIRT), which discovered the vulnerability, and allows hackers to launch local and remote attacks such as a denial-of-service (DoS) or a hijack of the affected system. Thompson Cyber Security Labs' director said attacks will become widespread because of the popularity of the exploit's NeoSploit toolkit delivery system. "The vulnerability is likely to be quite widespread, simply because of CA's size and spread within the corporate market," he said in his blog. "Corporate clients should probably be pretty nervous, because their firewall is unlikely to protect them against this."
Source: http://www.networkworld.com/news/2008/040108-new-exploit-targets-corporate-ca.html

29. *April 1, IDG News Service* – (International) **Cybercrime treaty gains more interest, momentum.** The number of countries that will have ratified the only international treaty addressing cybercrime is expected to nearly double this year, a sign that momentum is building behind efforts to police the Internet. The Council of Europe's Convention on Cybercrime, which sets guidelines for laws and procedures for dealing with Internet crime, was adopted in 2001. Countries can sign the treaty, which indicates their willingness to comply, and then can ratify it after their laws have been modified. So far, 22 countries have ratified the treaty, a lower number than expected since the treaty was introduced seven years ago, said the head of the economic crime division for the Council of Europe, on Tuesday. However, the Council hopes around 40 countries will ratify it by February 2009. The slow pace comes from the legal and legislative complexities that come with modifying laws in order to comply with the treaty, he said. The Council often works with countries to ensure their compliance. Countries outside the 47-member Council, which represents European countries, may apply for accession, the first step in implementing the treaty. The U.S., for example, has ratified the treaty, and more countries outside Europe are indicating their interest in joining, he said. The Convention is aimed at providing for swifter prosecutions of cybercrime as well as better cooperation between law enforcement agencies, as investigations often cross borders. For example, it requires countries to have a law enforcement contact available at all hours to assist in a digital investigation.
Source: http://www.networkworld.com/news/2008/040108-cybercrime-treaty-gains-more-interest.html

30. *April 1, IDG News Service* – (International) **Internet has a trash problem, researcher says.** Between one and three percent of all traffic on the Internet is meaningless packets of information, used in distributed denial of service attacks (DDOS) to knock Web sites offline. Those are the findings of Arbor Networks, a network traffic analysis company that recently looked at traffic flowing among more than 68 Internet service providers to see how much of it was malicious. **"**The thing that's surprising is it's consistently 1 to 3 percent," said Arbor's chief research officer. To purchase the bandwidth that Arbor tracked in these DDOS attacks, a legitimate user would have to pay hundreds of thousands of dollars per month, he said. That is not a problem for criminals, however, who use the network connections of their victims to attack others. DDOS attacks try to overwhelm the victim's servers with routine Internet messages. Attackers try to send so

many packets that the victim's computers are unable to do their regular jobs. They have become a common occurrence in recent years and have spawned a cottage industry of companies that try to mitigate their effects. Studying the data from about 1,300 routers over 18 months, Arbor found that the tidal waves of SYN (synchronization) or ICMP (Internet Control Message Protocol) packets used in DDOS attacks rarely dropped below one percent of all traffic and could easily rise to six percent during peak periods.
Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9074079&source=rss_topic17

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

31. *April 2, eWeek* – (International) **Research exposes vendor-specific VOIP vulnerabilities.** VOIPshield Systems on April 2 will seek to set itself apart among voice-over-IP security providers when it launches what officials claim is the first database of vulnerabilities specific to the IP PBXes of market leaders Cisco Systems, Avaya and Nortel Networks. "This is the first time a research lab will spell out what some of these vulnerabilities are," said the company's CEO. "We will announce them under the terms of our responsible disclosure policy. We first talked to the vendors and disclosed these, and we work with them and give any help they would like." "What's different about VOIPshield is their focus on [IP] telephony systems most commonly deployed at large enterprises in North America," said the research director of security and risk management at market research company Gartner. "Much of the focus with VOIP security to date is on [SIP (Session Initiation Protocols)], but when people roll out IP telephony today they are using proprietary signaling protocols that come with these PBXes," he said. VOIPshield through the two-year course of its research on the leading IP PBX systems found 144 different vulnerabilities across all three vendors' products, the company said. The 144 vulnerabilities are in four different categories of exploits, including denial of service, unauthorized access, information harvesting, and code execution.
Source: http://www.eweek.com/c/a/Security/Research-Exposes-Vendor-Specific-VOIP-Vulnerabilities/

32. *March 31, Telecoms* – (National) **Mobile fraud: Phone loving criminals**. Internet security firms, such as McAfee, Sophos and F-Secure, are making a lot of noise about the potential damage that malignant viruses, Tojans or other internet-style spam and scams will cause as they infiltrate the mobile handset population. Consumers can appreciate the potential for personal loss as they are well aware of the same issues in the

desktop environment. Meanwhile, the network and roaming vendors' primary concern is centered on various types of subscription and revenue share roaming fraud. Their public profile is a lot lower than the first set of vendors, since the subject area is of negligible concern to most consumers. Yet the costs for operators of these low-key frauds dwarf the costs incurred due to malware attacks. A global marketing manager at McAfee Mobile Security said: "A major share of fraud within a carrier is not caused by malicious content, like viruses and spyware, but by criminal activity such as roaming fraud and SIM card cloning. The biggest mobile security risks are also different carrier versus consumer." McAfee presented the results of its annual Mobile Security Report at this year's Mobile World Congress in Barcelona. The report, carried out in conjunction with analyst house Datamonitor, states that 86 per cent of the 2,000 mobile consumers it surveyed across the UK, US and Japan are worried about security risks posed to their mobile handset, with 79 per cent knowingly using unprotected devices. Consumers feel threatened, it seems, but not enough to do anything about it. The onus of responsibility, according to McAfee, falls with the operators. There is a chance that, if and when we move towards a fat pipe future with network agnostic devices, attitudes towards handset protection will change. For the foreseeable future though, operators must take the lead.
Source: http://www.telecoms.com/itmgcontent/tcoms/features/articles/20017518580.html

[Return to top]

Commercial Facilities Sector

Nothing to Report

[Return to top]

National Monuments & Icons Sector

33. *April 1, Associated Press* – (Oregon) **Vandals strike USS Portland monument on Portland's Eastern Prom.** Vandals marked up the monument to the USS Portland, which features part of the warship mainmast and bridge shield. They drew swastikas on it and left several references to Hitler. The USS Portland withstood attacks in several battles in the Pacific including Coral Sea, Midway, and Guadalcanal. Despite being torpedoed in 1942, it continued to fight even though a damaged rudder caused it to steam in circles in the Fourth Battle of Savo Island.
Source: http://www.wcsh6.com/news/article.aspx?storyid=83861

[Return to top]

Dams Sector

34. *April 1, WJAC 6 Johnstown* – (Pennsylvania) **DEP worried about Cold Stream Dam.** Pennsylvania's Department of Environmental Protection is worried about problems with Cold Stream Dam's spillway and flood plain; they say it could now be classified as a high hazard structure if flooding occurs. State officials want the dam to be brought into

compliance with updated regulations. Tuesday's meeting in Harrisburg reviewed alternatives and funding options to help pay for new construction.
Source: http://www.wjactv.com/news/15766799/detail.html

35. *April 1, KFVS 12 Cape Girardeau* – (Missouri) **Temporary levee protects Butler County.** It is sturdy enough to stand on, and hopefully strong enough to protect Butler County, Missouri, from more spring rain that could cause the Black River to rise again. It is an experimental, temporary levee brought in by the U.S. Army Corps of Engineers and installed around Poplar Bluff in the most vulnerable areas. The biggest break occurred nearly two weeks ago in the levee near County Road 606. It turned areas like Brosley and Qulin into a body of water that came to be known as Lake Butler County. It took 30 men less than a day to build the levee. The temporary levee is made of wire baskets covered in a felt-like material. They come flat, twist to open, and are then filled with sand and gravel.
Source: http://www.kfvs12.com/Global/story.asp?S=8097874

36. *April 1, Times-Picayune* – (Louisiana) **As the Mississippi River rises, Corps practices Spillway opening.** High atop the 77-year-old Bonnet Carre Spillway flood control structure, a seven-person work crew practiced opening the spillway to the Mississippi River on Tuesday. Fed by heavy rains in the Midwest, the river is rising and expected to crest April 8 at 16.5 feet at the Carrollton gauge in New Orleans, a half-foot below flood stage. However, Corps officials say they do not expect to have to open the spillway. Nevertheless, the possibility of more rain lent a little extra emphasis on the U.S. Army Corps of Engineers' annual drill to pull some of the wooden "needles" that seal off the spillway from the rising river. "Seal" is a loose term. When the river is high, water rushes through the gaps between the creosote-soaked pine boards that range from ten feet to 12 feet in length. On Tuesday, about 1,900 cubic feet per second of water was rushing through the structure, a fraction of its 250,000 cubic feet per second capacity. The Spillway Project manager said the drill is conducted every year so that workers can stay in practice lifting the 7,000 needles out of their bays with a crane and placing them on top of the structure.
Source:
http://www.nola.com/news/index.ssf/2008/04/as_water_rises_corps_practices.html

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-5389 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer